



Release Notes

FortiManager 7.4.1



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



August 31, 2023

FortiManager 7.4.1 Release Notes

02-741-927123-20230831

TABLE OF CONTENTS

Change Log	6
FortiManager 7.4.1 Release	7
Supported models	7
FortiManager VM subscription license	7
Management extension applications	7
Supported models for MEA	8
Minimum system requirements	8
Special Notices	10
Serial console has changed for FortiManager deployments on Xen	10
OpenXen in PV mode is not supported in FortiManager 7.4.1	10
Default GUI theme changed	10
Management Extensions visibility in the GUI	10
Install On column for policies	10
SD-WAN Orchestrator removed in 7.2	11
Changes to FortiManager meta fields	11
Setup wizard requires FortiCare registration	11
Access lists as ADOM-level objects	11
View Mode is disabled in policies when policy blocks are used	11
Reconfiguring Virtual Wire Pairs (VWP)	12
Scheduling firmware upgrades for managed devices	12
Modifying the interface status with the CLI	12
SD-WAN with upgrade to 7.0	12
Citrix XenServer default limits and upgrade	12
Multi-step firmware upgrades	13
Hyper-V FortiManager-VM running on an AMD CPU	13
SSLv3 on FortiManager-VM64-AWS	13
Upgrade Information	14
Downgrading to previous firmware versions	14
Firmware image checksums	14
FortiManager VM firmware	15
SNMP MIB files	16
Product Integration and Support	17
Supported software	17
Web browsers	18
FortiOS and FortiOS Carrier	18
FortiADC	18
FortiAnalyzer	18
FortiAnalyzer-BigData	19
FortiAuthenticator	19
FortiCache	19
FortiCASB	19
FortiClient	19

FortiDDoS	19
FortiDeceptor	20
FortiFirewall and FortiFirewallCarrier	20
FortiMail	20
FortiPAM	20
FortiProxy	20
FortiSandbox	21
FortiSOAR	21
FortiSwitch ATCA	21
FortiTester	21
FortiToken	21
FortiWeb	22
Virtualization	22
Feature support	22
Language support	23
Supported models	24
FortiGate models	24
FortiGate special branch models	27
FortiCarrier models	28
FortiCarrier special branch models	30
FortiADC models	31
FortiAnalyzer models	31
FortiAnalyzer-BigData models	32
FortiAuthenticator models	32
FortiCache models	33
FortiDDoS models	33
FortiDeceptor models	33
FortiFirewall models	33
FortiFirewallCarrier models	34
FortiMail models	35
FortiPAM models	35
FortiProxy models	35
FortiSandbox models	36
FortiSOAR models	36
FortiSwitch ATCA models	36
FortiTester models	36
FortiWeb models	37
Resolved Issues	38
AP Manager	38
Device Manager	38
FortiSwitch Manager	39
Global ADOM	39
Others	40
Policy and Objects	40
Revision History	42
Script	42
System Settings	42

VPN Manager	43
Known Issues	44
AP Manager	44
Device Manager	44
FortiSwitch Manager	44
Others	45
Policy & Objects	45
Revision History	46
System Settings	46
VPN Manager	46
Appendix A - FortiGuard Distribution Servers (FDS)	47
FortiGuard Center update support	47
Appendix B - Default and maximum number of ADOMs supported	48
Hardware models	48
Virtual Machines	48

Change Log

Date	Change Description
2023-08-31	Initial release.

FortiManager 7.4.1 Release

This document provides information about FortiManager version 7.4.1 build 2308.



The recommended minimum screen resolution for the FortiManager GUI is 1920 x 1080. Please adjust the screen resolution accordingly. Otherwise, the GUI may not display properly.

This section includes the following topics:

- [Supported models on page 7](#)
- [FortiManager VM subscription license on page 7](#)
- [Management extension applications on page 7](#)

Supported models

FortiManager version 7.4.1 supports the following models:

FortiManager	FMG-200F, FMG-200G, FMG-300F, FMG-400E, FMG-400G, FMG-1000F, FMG-2000E FMG-3000F, FMG-3000G, FMG-3700F, and FMG-3700G.
FortiManager VM	FMG_DOCKER, FMG_VM64, FMG_VM64_ALI, FMG_VM64_AWS, FMG_VM64_AWSOnDemand, FMG_VM64_Azure, FMG_VM64_GCP, FMG_VM64_IBM, FMG_VM64_HV (including Hyper-V 2016, 2019), FMG_VM64_KVM, FMG_VM64_OPC, FMG_VM64_XEN (for both Citrix and Open Source Xen).

FortiManager VM subscription license

The FortiManager VM subscription license supports FortiManager version 6.4.1 and later. For information about supported firmware, see [FortiManager VM firmware on page 15](#).

See also [Appendix B - Default and maximum number of ADOMs supported on page 48](#).

Management extension applications

The following section describes supported models and minimum system requirements for management extension applications (MEA) in FortiManager 7.4.1.



FortiManager uses port TCP/443 or TCP/4443 to connect to the Fortinet registry and download MEAs. Ensure that the port is also open on any upstream FortiGates. For more information about incoming and outgoing ports, see the [FortiManager 7.0 Ports Guide](#).

As of FortiManager 7.4.0, the *Management Extensions* pane is only visible in the GUI when docker status is enabled and at least one MEA is enabled and downloaded. For more information about enabling and using the MEAs, see the Management Extensions documentation in the [FortiManager Documents Library](#).

Supported models for MEA

You can use any of the following FortiManager models as a host for management extension applications:

FortiManager	FMG-3000F, FMG-3000G, FMG-3700F, and FMG-3700G.
FortiManager VM	FMG_DOCKER, FMG_VM64, FMG_VM64_ALI, FMG_VM64_AWS, FMG_VM64_AWSOnDemand, FMG_VM64_Azure, FMG_VM64_GCP, FMG_VM64_IBM, FMG_VM64_HV (including Hyper-V 2016, 2019), FMG_VM64_KVM, FMG_VM64_OPC, FMG_VM64_XEN (for both Citrix and Open Source Xen).

Minimum system requirements

By default FortiManager VMs use the following system resource settings:

- 4 vCPU
- 8 GB RAM
- 500 GB disk space

Starting with FortiManager 7.0.0, RAM and CPU is capped at 50% for MEAs. (Use the `config system docker` command to view the setting.) If FortiManager has 8 CPUs and 16 GB RAM, then only 4 CPUs and 8 GB RAM are available to MEAs by default, and the 4 CPUs and 8 GB RAM are used for all enabled MEAs.

Some management extension applications have minimum system requirements that require you to increase system resources. The following table identifies the minimum requirements for each MEA as well as the recommended system resources to function well in a production environment.

MEA minimum system requirements apply only to the individual MEA and do not take into consideration any system requirements for resource-sensitive FortiManager features or multiple, enabled MEAs. If you are using multiple MEAs, you must increase the system resources to meet the cumulative need of each MEA.

Management Extension Application	Minimum system requirements	Recommended system resources for production*
FortiAIOps	<ul style="list-style-type: none"> • 8 vCPU • 32 GB RAM • 500 GB disk storage 	No change
FortiSigConverter	<ul style="list-style-type: none"> • 4 vCPU • 8 GB RAM 	No change

Management Extension Application	Minimum system requirements	Recommended system resources for production*
FortiSOAR	<ul style="list-style-type: none"> • 4 vCPU • 8 GB RAM • 500 GB disk storage 	<ul style="list-style-type: none"> • 16 vCPU • 64 GB RAM • No change for disk storage
Policy Analyzer	<ul style="list-style-type: none"> • 4 vCPU • 8 GB RAM 	No change
Universal Connector	<ul style="list-style-type: none"> • 1 GHZ vCPU • 2 GB RAM • 1 GB disk storage 	No change
Wireless Manager (FortiWLM)	<ul style="list-style-type: none"> • 4 vCPU • 8 GB RAM 	No change

*The numbers in the *Recommended system resources for production* column are a combination of the default system resource settings for FortiManager plus the minimum system requirements for the MEA.

Special Notices

This section highlights some of the operational changes that administrators should be aware of in 7.4.1.

Serial console has changed for FortiManager deployments on Xen

As of FortiManager 7.4.1, the serial console for Xen deployments has changed from hvc0 (Xen specific) to ttyS0 (standard).

OpenXen in PV mode is not supported in FortiManager 7.4.1

As of FortiManager 7.4.1, kernel and rootfs are encrypted. OpenXen in PV mode tries to unzip the kernel and rootfs, but it will fail. Therefore, OpenXen in PV mode cannot be used when deploying or upgrading to FortiManager 7.4.1. Only HVM (hardware virtual machine) mode is supported for OpenXen in FortiManager 7.4.1.

Default GUI theme changed

As of FortiManager 7.4.1, the default GUI theme is *Jade*. The default theme can be changed from *System Settings > Settings*.

Management Extensions visibility in the GUI

As of FortiManager 7.4.0, the *Management Extensions* pane is only visible in the GUI when docker status is enabled and at least one management extension application (MEA) is enabled and downloaded. For more information about enabling and using the MEAs, see the Management Extensions documentation in the [FortiManager Documents Library](#).

Install On column for policies

Prior to version 7.2.3, the 'Install-on' column for policies in the policy block had no effect. However, starting from version 7.2.3, the 'Install-on' column is operational and significantly impacts the behavior and installation process of policies. It's important to note that using 'Install-on' on policies in the policy block is not recommended. If required, this setting can only be configured through a script or JSON APIs.

SD-WAN Orchestrator removed in 7.2

Starting in 7.2.0, the SD-WAN Orchestrator is no longer available in FortiManager. Instead, you can use the *SD-WAN Overlay Template* wizard to configure your SD-WAN overlay network.

For more information, see [SD-WAN Overlay Templates](#) in the FortiManager Administration Guide.

Changes to FortiManager meta fields

Beginning in 7.2.0, FortiManager supports policy object metadata variables.

When upgrading from FortiManager 7.0 to 7.2.0 and later, FortiManager will automatically create ADOM-level metadata variable policy objects for meta fields previously configured in System Settings that have per-device mapping configurations detected. Objects using the meta field, for example CLI templates, are automatically updated to use the new metadata variable policy objects.

Meta fields in *System Settings* can continue to be used as comments/tags for configurations.

For more information, see [ADOM-level meta variables for general use in scripts, templates, and model devices](#).

Setup wizard requires FortiCare registration

Starting in FortiManager 7.2.1, the FortiManager Setup wizard requires you to complete the *Register with FortiCare* step before you can access the FortiManager appliance or VM. Previously the step was optional.

For FortiManager units operating in a closed environment, contact customer service to receive an entitlement file, and then load the entitlement file to FortiManager by using the CLI.

Access lists as ADOM-level objects

Starting in 7.2.0, FortiManager supports IPv4 and IPv6 access lists as ADOM-level object configurations from FortiGate. Previously, access lists were controlled by the device database/FortiGate configuration.

After upgrading to 7.2.0 from an earlier release, the next time you install changes to a FortiGate device with an IPv4 or IPv6 access list, FortiManager will purge the device database/FortiGate configuration which may have previously contained the access list. To address this, administrators can re-import the FortiGate policy configuration to an ADOM's policy package or re-create the IPv4/IPv6 access list in the original package.

View Mode is disabled in policies when policy blocks are used

When policy blocks are added to a policy package, the *View Mode* option is no longer available, and policies in the table cannot be arranged by *Interface Pair View*. This occurs because policy blocks typically contain policies with multiple

interfaces, however, *View Mode* is still disabled even when policy blocks respect the interface pair.

Reconfiguring Virtual Wire Pairs (VWP)

A conflict can occur between the ADOM database and device database when a Virtual Wire Pair (VWP) is installed on a managed FortiGate that already has a configured VWP in the device database. This can happen when an existing VWP has been reconfigured or replaced.

Before installing the VWP, you must first remove the old VWP from the device's database, otherwise a policy and object validation error may occur during installation. You can remove the VWP from the device database by going to *Device Manager > Device & Groups*, selecting the managed device, and removing the VWP from *System > Interface*.

Scheduling firmware upgrades for managed devices

Starting in FortiManager 7.0.0, firmware templates should be used to schedule firmware upgrades on managed FortiGates. Attempting firmware upgrade from the FortiManager GUI by using legacy methods may ignore the *schedule upgrade* option and result in FortiGates being upgraded immediately.

Modifying the interface status with the CLI

Starting in version 7.0.1, the CLI to modify the interface status has been changed from *up/down* to *enable/disable*.

For example:

```
config system interface
  edit port2
    set status <enable/disable>
  next
end
```

SD-WAN with upgrade to 7.0

Due to design change with SD-WAN Template, upgrading to FortiManager 7.0 may be unable to maintain dynamic mappings for all SD-WAN interface members. Please reconfigure all the missing interface mappings after upgrade.

Citrix XenServer default limits and upgrade

Citrix XenServer limits ramdisk to 128M by default. However the FMG-VM64-XEN image is larger than 128M. Before updating to FortiManager 6.4, increase the size of the ramdisk setting on Citrix XenServer.

To increase the size of the ramdisk setting:

1. On Citrix XenServer, run the following command:
`xenstore-write /mh/limits/pv-ramdisk-max-size 536,870,912`
2. Confirm the setting is in effect by running `xenstore-ls`.

`limits = ""`
`pv-kernel-max-size = "33554432"`
`pv-ramdisk-max-size = "536,870,912"`
`boot-time = ""`

3. Remove the pending files left in `/run/xen/pygrub`.



The ramdisk setting returns to the default value after rebooting.

Multi-step firmware upgrades

Prior to using the FortiManager to push a multi-step firmware upgrade, confirm the upgrade path matches the path outlined on our support site. To confirm the path, please run:

```
dia fwmanager show-dev-upgrade-path <device name> <target firmware>
```

Alternatively, you can push one firmware step at a time.

Hyper-V FortiManager-VM running on an AMD CPU

A Hyper-V FMG-VM running on a PC with an AMD CPU may experience a kernel panic. Fortinet recommends running VMs on an Intel-based PC.

SSLv3 on FortiManager-VM64-AWS

Due to known vulnerabilities in the SSLv3 protocol, FortiManager-VM64-AWS only enables TLSv1 by default. All other models enable both TLSv1 and SSLv3. If you wish to disable SSLv3 support, please run:

```
config system global
set ssl-protocol tlsv1
end
```

Upgrade Information



Prior to upgrading your FortiManager, please review the FortiManager Upgrade Guide in detail as it includes all of the necessary steps and associated details required to upgrade your FortiManager device or VM.

See the *FortiManager Upgrade Guide* in the [Fortinet Document Library](#).

You can upgrade FortiManager 7.2.0 or later directly to 7.4.1.



Before upgrading FortiManager, check ADOM versions. Check the ADOM versions supported by the destination firmware and the current firmware. If the current firmware uses ADOM versions not supported by the destination firmware, upgrade ADOM versions in FortiManager before upgrading FortiManager to the destination firmware version.

For example, FortiManager 7.2 supports ADOM versions 6.4, 7.0, and 7.2, but FortiManager 7.4 supports ADOM versions 7.0, 7.2, and 7.4. Before you upgrade FortiManager 7.2 to 7.4, ensure that all ADOM 6.4 versions have been upgraded to ADOM version 7.0 or later. See the *FortiManager Upgrade Guide* in the [Fortinet Document Library](#).

This section contains the following topics:

- [Downgrading to previous firmware versions on page 14](#)
- [Firmware image checksums on page 14](#)
- [FortiManager VM firmware on page 15](#)
- [SNMP MIB files on page 16](#)

Downgrading to previous firmware versions

FortiManager does not provide a full downgrade path. You can downgrade to a previous firmware release by using the GUI or CLI, but doing so results in configuration loss. A system reset is required after the firmware downgrade process has completed. To reset the system, use the following CLI commands via a console port connection:

```
execute reset {all-settings | all-except-ip}  
execute format {disk | disk-ext4 | disk-ext3}
```

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, <https://support.fortinet.com>. After logging in, go to *Download > Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

FortiManager VM firmware

Fortinet provides FortiManager VM firmware images for Amazon AWS, Amazon AWSOnDemand, Citrix and Open Source XenServer, Linux KVM, Microsoft Hyper-V Server, and VMware ESX/ESXi virtualization environments.

Amazon Web Services

- The 64-bit Amazon Machine Image (AMI) is available on the AWS marketplace.

Citrix XenServer and Open Source XenServer

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiManager VM installation. This package contains the QCOW2 file for the Open Source Xen Server.
- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiManager VM installation. This package contains the Citrix XenServer Virtual Appliance (XVA), Virtual Hard Disk (VHD), and OVF files.

Google Cloud Platform

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.gcp.zip`: Download the 64-bit package for a new FortiManager VM installation.

Linux KVM

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiManager VM installation. This package contains QCOW2 that can be used by qemu.

Microsoft Azure

The files for Microsoft Azure have AZURE in the filenames, for example `<product>_VM64_AZURE-v<number>-build<number>-FORTINET.out.hyperv.zip`.

- `.out`: Download the firmware image to upgrade your existing FortiManager VM installation.

Microsoft Hyper-V Server

The files for Microsoft Hyper-V Server have HV in the filenames, for example, `<product>_VM64_HV-v<number>-build<number>-FORTINET.out.hyperv.zip`.

- `.out`: Download the firmware image to upgrade your existing FortiManager VM installation.
- `.hyperv.zip`: Download the package for a new FortiManager VM installation. This package contains a Virtual Hard Disk (VHD) file for Microsoft Hyper-V Server.



Microsoft Hyper-V 2016 is supported.

Oracle Private Cloud

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiManager VM installation.
- `.out.opc.zip`: Download the 64-bit package for a new FortiManager VM installation.

VMware ESX/ESXi

- `.out`: Download the 64-bit firmware image to upgrade your existing VM installation.
- `.ovf.zip`: Download either the 64-bit package for a new VM installation. This package contains an Open Virtualization Format (OVF) file for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.



For more information see the [FortiManager Data Sheet](#) available on the Fortinet web site. VM installation guides are available in the [Fortinet Document Library](#).

SNMP MIB files

You can download the *FORTINET-FORTIMANAGER-FORTIANALYZER.mib* MIB file in the firmware image file folder. The Fortinet Core MIB file is located in the main FortiManager version 5.00 file folder.

Product Integration and Support

This section lists FortiManager 7.4.1 support of other Fortinet products. It also identifies what FortiManager features are supported for managed platforms and what languages FortiManager supports. It also lists which Fortinet models can be managed by FortiManager.

The section contains the following topics:

- [Supported software on page 17](#)
- [Feature support on page 22](#)
- [Language support on page 23](#)
- [Supported models on page 24](#)

Supported software

FortiManager 7.4.1 supports the following software:

- [Web browsers on page 18](#)
- [FortiOS and FortiOS Carrier on page 18](#)
- [FortiADC on page 18](#)
- [FortiAnalyzer on page 18](#)
- [FortiAnalyzer-BigData on page 19](#)
- [FortiAuthenticator on page 19](#)
- [FortiCache on page 19](#)
- [FortiCASB on page 19](#)
- [FortiClient on page 19](#)
- [FortiDDoS on page 19](#)
- [FortiDeceptor on page 20](#)
- [FortiFirewall and FortiFirewallCarrier on page 20](#)
- [FortiMail on page 20](#)
- [FortiPAM on page 20](#)
- [FortiProxy on page 20](#)
- [FortiSandbox on page 21](#)
- [FortiSOAR on page 21](#)
- [FortiSwitch ATCA on page 21](#)
- [FortiTester on page 21](#)
- [FortiToken on page 21](#)
- [FortiWeb on page 22](#)
- [Virtualization on page 22](#)



To confirm that a device model or firmware version is supported by the current firmware version running on FortiManager, run the following CLI command:

```
diagnose dvm supported-platforms list
```



Always review the Release Notes of the supported platform firmware version before upgrading your device.

Web browsers

FortiManager 7.4.1 supports the following web browsers:

- Microsoft Edge 114
- Mozilla Firefox version 96
- Google Chrome version 114

Other web browsers may function correctly, but are not supported by Fortinet.

FortiOS and FortiOS Carrier



The *FortiManager Release Notes* communicate support for FortiOS versions that are available at the time of the FortiManager 7.4.1 release. For additional information about other supported FortiOS versions, please refer to the FortiManager compatibility chart in the [Fortinet Document Library](#).

See [FortiManager compatibility with FortiOS](#).

FortiManager 7.4.1 supports the following versions of FortiOS and FortiOS Carrier:

- 7.4.0 to 7.4.1
- 7.2.0 to 7.2.5
- 7.0.0 to 7.0.12

FortiADC

FortiManager 7.4.1 supports the following versions of FortiADC:

- 7.4.0 and later
- 7.2.0 and later
- 7.1.0 and later

FortiAnalyzer

FortiManager 7.4.1 supports the following versions of FortiAnalyzer:

- 7.4.0
- 7.2.0 and later
- 7.0.0 and later

FortiAnalyzer-BigData

FortiManager 7.4.1 supports the following versions of FortiAnalyzer-BigData:

- 7.2.0 and later
- 7.0.0 and later

FortiAuthenticator

FortiManager 7.4.1 supports the following versions of FortiAuthenticator:

- 6.5.0 and later
- 6.4.0 and later
- 6.3.0 and later

FortiCache

FortiManager 7.4.1 supports the following versions of FortiCache:

- 4.2.0 and later
- 4.1.0 and later
- 4.0.0 and later

FortiCASB

FortiManager 7.4.1 supports the following versions of FortiCASB:

- 23.2.0 and later

FortiClient

FortiManager 7.4.1 supports the following versions of FortiClient:

- 7.2.0 and later
- 7.0.0 and later
- 6.4.0 and later

FortiDDoS

FortiManager 7.4.1 supports the following versions of FortiDDoS:

- 6.5.0 and later
- 6.4.0 and later
- 6.3.0 and later

Limited support. For more information, see [Feature support on page 22](#).

FortiDeceptor

FortiManager 7.4.1 supports the following versions of FortiDeceptor:

- 5.1.0 and later
- 5.0.0 and later
- 4.3.0 and later

FortiFirewall and FortiFirewallCarrier

FortiManager 7.4.1 supports the following versions of FortiFirewall and FortiFirewallCarrier:

- 7.4.0 and later
- 7.2.0 and later
- 7.0.0 and later

FortiMail

FortiManager 7.4.1 supports the following versions of FortiMail:

- 7.4.0 and later
- 7.2.0 and later
- 7.0.0 and later

FortiPAM

FortiManager 7.4.1 supports the following versions of FortiPAM:

- 1.1.0 and later
- 1.0.0 and later

FortiProxy

FortiManager 7.4.1 supports configuration management for the following versions of FortiProxy:

- 7.2.3
- 7.2.2
- 7.0.7



Configuration management support is identified as *Management Features* in these release notes. See [Feature support on page 22](#).

FortiManager 7.4.1 supports logs from the following versions of FortiProxy:

- 7.4.0
7.2.0 to 7.2.5

- 7.0.0 to 7.0.11
- 2.0.0 to 2.0.5
- 1.2.0 to 1.2.13
- 1.1.0 to 1.1.6
- 1.0.0 to 1.0.7

FortiSandbox

FortiManager 7.4.1 supports the following versions of FortiSandbox:

- 4.2.0 and later
- 4.0.0 and 4.0.1
- 3.2.0 and later

FortiSOAR

FortiManager 7.4.1 supports the following versions of FortiSOAR:

- 7.4.0 and later
- 7.3.0 and later
- 7.2.0 and later

FortiSwitch ATCA

FortiManager 7.4.1 supports the following versions of FortiSwitch ATCA:

- 5.2.0 and later
- 5.0.0 and later
- 4.3.0 and later

FortiTester

FortiManager 7.4.1 supports the following versions of FortiTester:

- 7.2.0 and later
- 7.1.0 and later
- 7.0.0 and later

FortiToken

FortiManager 7.4.1 supports the following versions of FortiToken:

- 3.0.0 and later

FortiWeb

FortiManager 7.4.1 supports the following versions of FortiWeb:

- 7.2.0 and later
- 7.0.0 and later
- 6.4.0 and later
- 6.3.0 and later

Virtualization

FortiManager 7.4.1 supports the following virtualization software:

- Amazon Web Service AMI, Amazon EC2, Amazon EBS
- Citrix XenServer 7.2
- Google Cloud Platform
- Linux KVM Redhat 7.1
- Microsoft Azure
- Microsoft Hyper-V Server 2012, 2016, and 2019
- Nutanix AHV (AOS 5.10.5)
- OpenSource XenServer 4.2.5
- Oracle Private Cloud
- VMware ESXi versions 6.5 and later

Feature support

The following table lists FortiManager feature support for managed platforms.

Platform	Management Features	FortiGuard Update Services	VM License Activation	Reports	Logging
FortiGate	✓	✓	✓	✓	✓
FortiCarrier	✓	✓	✓	✓	✓
FortiADC		✓	✓		
FortiAnalyzer			✓	✓	✓
FortiAuthenticator					✓
FortiCache			✓	✓	✓
FortiClient		✓		✓	✓
FortiDDoS			✓	✓	✓
FortiDeceptor		✓			

Platform	Management Features	FortiGuard Update Services	VM License Activation	Reports	Logging
FortiFirewall	✓				✓
FortiFirewall Carrier	✓				✓
FortiMail		✓	✓	✓	✓
FortiProxy	✓	✓	✓	✓	✓
FortiSandbox		✓	✓	✓	✓
FortiSOAR		✓	✓		
FortiSwitch ATCA	✓				
FortiTester		✓			
FortiWeb		✓	✓	✓	✓
Syslog					✓

Language support

The following table lists FortiManager language support information.

Language	GUI	Reports
English	✓	✓
Chinese (Simplified)	✓	✓
Chinese (Traditional)	✓	✓
French	✓	✓
Japanese	✓	✓
Korean	✓	✓
Portuguese		✓
Spanish		✓

To change the FortiManager language setting, go to *System Settings > Admin > Admin Settings*, in *Administrative Settings > Language* select the desired language on the drop-down menu. The default value is *Auto Detect*.

Russian, Hebrew, and Hungarian are not included in the default report languages. You can create your own language translation files for these languages by exporting a predefined language from FortiManager, modifying the text to a different language, saving the file as a different language name, and then importing the file into FortiManager. For more information, see the *FortiManager Administration Guide*.

Supported models

The following tables list which FortiGate, FortiCarrier, FortiDDoS, FortiAnalyzer, FortiMail, FortiSandbox, FortiSwitch ATCA, FortiWeb, FortiCache, FortiProxy, and FortiAuthenticator models and firmware versions that can be managed by a FortiManager or send logs to a FortiManager running version 7.4.1.



Software license activated LENC devices are supported, if their platforms are in the supported models list. For example, support of FG-3200D indicates support of FG-3200D-LENC.

This section contains the following topics:

- [FortiGate models on page 24](#)
- [FortiGate special branch models on page 27](#)
- [FortiCarrier models on page 28](#)
- [FortiCarrier special branch models on page 30](#)
- [FortiADC models on page 31](#)
- [FortiAnalyzer models on page 31](#)
- [FortiAnalyzer-BigData models on page 32](#)
- [FortiAuthenticator models on page 32](#)
- [FortiCache models on page 33](#)
- [FortiDDoS models on page 33](#)
- [FortiDeceptor models on page 33](#)
- [FortiFirewall models on page 33](#)
- [FortiFirewallCarrier models on page 34](#)
- [FortiMail models on page 35](#)
- [FortiPAM models on page 35](#)
- [FortiProxy models on page 35](#)
- [FortiSandbox models on page 36](#)
- [FortiSOAR models on page 36](#)
- [FortiSwitch ATCA models on page 36](#)
- [FortiTester models on page 36](#)
- [FortiWeb models on page 37](#)

FortiGate models

The following FortiGate models are released with FortiOS firmware. For information about supported FortiGate models on special branch releases of FortiOS firmware, see [FortiGate special branch models on page 27](#).



The following FortiGate models are not supported in 7.4 by FortiManager 7.4.0 due to FortiOS syntax issues:

- FortiGate-91E
 - FortiGateRugged-70F/70F-3G4G
-

Model	Firmware Version
FortiGate: FortiGate-40F, FortiGate-40F-3G4G, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-70F, FortiGate-71F, FortiGate-80E, FortiGate-80E-POE, FortiGate-80F, FortiGate-80F-Bypass, FortiGate-80F-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-81F, FortiGate-81F-POE, FortiGate-90E, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-200F, FortiGate-201E, FortiGate-201F, FortiGate-300E, FortiGate-301E, FortiGate-400E, FortiGate-400F, FortiGate-400E-Bypass, FortiGate-401E, FortiGate-401F, FortiGate-500E, FortiGate-501E, FortiGate-600E, FortiGate-600F, FortiGate-601E, FortiGate-601F, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1100E, FortiGate-1101E, FortiGate-1500D, FortiGate-1500DT, FortiGate-1800F, FortiGate-1801F, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-2600F, FortiGate-2601F, FortiGate-3000D, FortiGate-3000F, FortiGate-3001F, FortiGate-3100D, FortiGate-3200D, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3500F, FortiGate-3501F, FortiGate-3600E, FortiGate-3600E-DC, FortiGate-3601E, FortiGate-3700D, FortiGate-3800D, FortiGate-3960E, FortiGate-3980E, FortiGate-4200F, FortiGate-4201F, FortiGate-4400F, FortiGate-4401F FortiGate 5000 Series: FortiGate-5001E, FortiGate-5001E1 FortiGate 6000 Series: FortiGate-6000F, FortiGate-6300F, FortiGate-6300F-DC, FortiGate-6301F, FortiGate-6301F-DC, FortiGate-6500F, FortiGate-6500F-DC, FortiGate-6501F, FortiGate-6501F-DC FortiGate 7000 Series: FortiGate-7000E, FortiGate-7000F, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC, FortiGate-7081F, FortiGate-7121F, FortiGate-7121F-2, FortiGate-7121F-2-DC, FortiGate-7121F-DC FortiGate DC: FortiGate-401E-DC, FortiGate-800D-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-1800F-DC, FortiGate-1801F-DC, FortiGate-2201E-ACDC, FortiGate-2600F-DC, FortiGate-2601F-DC, FortiGate-3000D-DC, FortiGate-3000F-DC, FortiGate-3001F-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3400E-DC, FortiGate-3401E-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3960E-ACDC, FortiGate-3960E-DC, FortiGate-3980E-DC, FortiGate-4200F-DC, FortiGate-4201F-DC, FortiGate-4400F-DC, FortiGate-4401F-DC FortiWiFi: FWF-40F, FWF-40F-3G4G, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-80F-2R, FWF-81F-2R, FWF-81F-2R-3G4G-POE, FWF-81F-2R-POE FortiGate VM: FortiGate-ARM64-AWS, FortiGate-ARM64-Azure, FortiGate-ARM64-GCP, FortiGate-ARM64-KVM, FortiGate-ARM64-OCI, FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-AWS, FortiGate-VM64-Azure, FortiGate-VM64-GCP, FortiGate-VM64-HV, FortiGate-VM64-IBM, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-RAXONDEMAND, FortiGate-VM64-Xen FortiGate Rugged: FGR-60F, FGR-60F-3G4G, FGR-70F, FGR-70F-3G4G	7.4

Model	Firmware Version
FortiGate: FortiGate-40F, FortiGate-40F-3G4G, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-70F, FortiGate-71F, FortiGate-80E, FortiGate-80E-POE, FortiGate-80F, FortiGate-80F-Bypass, FortiGate-80F-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-81F, FortiGate-81F-POE, FortiGate-90E, FortiGate-91E, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-200F, FortiGate-201E, FortiGate-201F, FortiGate-300E, FortiGate-301E, FortiGate-400E, FortiGate-400E-Bypass, FortiGate-400F, FortiGate-401E, FortiGate-401F, FortiGate-500E, FortiGate-501E, FortiGate-600E, FortiGate-600F, FortiGate-601E, FortiGate-601F, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1100E, FortiGate-1101E, FortiGate-1500D, FortiGate-1500DT, FortiGate-1800F, FortiGate-1801F, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-2600F, FortiGate-2601F, FortiGate-3000D, FortiGate-3000F, FortiGate-3001F, FortiGate-3100D, FortiGate-3200D, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3500F, FortiGate-3501F, FortiGate-3600E, FortiGate-3601E, FortiGate-3700D, FortiGate-3800D, FortiGate-3960E, FortiGate-3980E, FortiGate-4200F, FortiGate-4201F, FortiGate-4400F, FortiGate-4401F FortiGate 5000 Series: FortiGate-5001E, FortiGate-5001E1 FortiGate 6000 Series: FortiGate-6000F, FortiGate-6300F, FortiGate-6300F-DC, FortiGate-6301F, FortiGate-6301F-DC, FortiGate-6500F, FortiGate-6500F-DC, FortiGate-6501F, FortiGate-6501F-DC FortiGate 7000 Series: FortiGate-7000E, FortiGate-7000F, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC, FortiGate-7081F, FortiGate-7121F, FortiGate-7121F-2, FortiGate-7121F-2-DC, FortiGate-7121F-DC FortiGate DC: FortiGate-401E-DC, FortiGate-800D-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-1800F-DC, FortiGate-1801F-DC, FortiGate-2201E-ACDC, FortiGate-2600F-DC, FortiGate-2601F-DC, FortiGate-3000D-DC, FortiGate-3000F-DC, FortiGate-3001F-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3400E-DC, FortiGate-3401E-DC, FortiGate-3600E-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3960E-ACDC, FortiGate-3960E-DC, FortiGate-3980E-DC, FortiGate-4200F-DC, FortiGate-4201F-DC, FortiGate-4400F-DC, FortiGate-4401F-DC FortiWiFi: FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-80F-2R, FWF-81F-2R, FWF-81F-2R-3G4G-POE, FWF-81F-2R-POE FortiGate VM: FortiGate-ARM64-AWS, FortiGate-ARM64-Azure, FortiGate-ARM64-GCP, FortiGate-ARM64-KVM, FortiGate-ARM64-OCI, FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-AWS, FortiGate-VM64-Azure, FortiGate-VM64-GCP, FortiGate-VM64-HV, FortiGate-VM64-IBM, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-RAXONDEMAND, FortiGate-VM64-XEN, FortiGate-VMX-Service-Manager FortiOS-VM: FOS-VM64, FOS-VM64-HV, FOS-VM64-KVM, FOS-VM64-Xen FortiGate Rugged: FGR-60F, FGR-60F-3G4G	7.2

Model	Firmware Version
FortiGate: FortiGate-40F, FortiGate-40F-3G4G, FortiGate-60E, FortiGate-60E-DSL, FortiGate-60E-DSLJ, FortiGate-60E-POE, FortiGate-60F, FortiGate-61E, FortiGate-61F, FortiGate-70F, FortiGate-71F, FortiGate-80E, FortiGate-80E-POE, FortiGate-80F, FortiGate-80F-Bypass, FortiGate-80F-POE, FortiGate-81E, FortiGate-81E-POE, FortiGate-81F, FortiGate-81F-POE, FortiGate-90E, FortiGate-91E, FortiGate-100E, FortiGate-100EF, FortiGate-100F, FortiGate-101E, FortiGate-101F, FortiGate-140E, FortiGate-140E-POE, FortiGate-200E, FortiGate-200F, FortiGate-201E, FortiGate-201F, FortiGate-300D, FortiGate-300E, FortiGate-301E, FortiGate-400D, FortiGate-400E, FortiGate-400E-Bypass, FortiGate-400F, FortiGate-401E, FortiGate-401F, FortiGate-500D, FortiGate-500E, FortiGate-501E, FortiGate-600D, FortiGate-600E, FortiGate-600F, FortiGate-601E, FortiGate-601F, FortiGate-800D, FortiGate-900D, FortiGate-1000D, FortiGate-1100E, FortiGate-1101E, FortiGate-1200D, FortiGate-1500D, FortiGate-1500DT, FortiGate-1800F, FortiGate-1801F, FortiGate-2000E, FortiGate-2200E, FortiGate-2201E, FortiGate-2500E, FortiGate-2600F, FortiGate-2601F, FortiGate-3000D, FortiGate-3000F, FortiGate-3001F, FortiGate-3100D, FortiGate-3200D, FortiGate-3300E, FortiGate-3301E, FortiGate-3400E, FortiGate-3401E, FortiGate-3500F, FortiGate-3501F, FortiGate-3600E, FortiGate-3601E, FortiGate-3700D, FortiGate-3800D, FortiGate-3810D, FortiGate-3815D, FortiGate-3960E, FortiGate-3980E, FortiGate-4200F, FortiGate-4201F, FortiGate-4400F, FortiGate-4401F, FortiGate 5000 Series: FortiGate-5001D, FortiGate-5001E, FortiGate-5001E1 FortiGate DC: FortiGate-401E-DC, FortiGate-800D-DC, FortiGate-1100E-DC, FortiGate-1500D-DC, FortiGate-1800F-DC, FortiGate-1801F-DC, FortiGate-2201E-ACDC, FortiGate-2600F-DC, FortiGate-2601F-DC, FortiGate-3000D-DC, FortiGate-3000F-DC, FortiGate-3001F-DC, FortiGate-3100D-DC, FortiGate-3200D-DC, FortiGate-3400E-DC, FortiGate-3401E-DC, FortiGate-3600E-DC, FortiGate-3700D-DC, FortiGate-3800D-DC, FortiGate-3810D-DC, FortiGate-3815D-DC, FortiGate-3960E-ACDC, FortiGate-3960E-DC, FortiGate-3980E-DC, FortiGate-4200F-DC, FortiGate-4201F-DC, FortiGate-4400F-DC, FortiGate-4401F-DC FortiWiFi: FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-80F-2R, FWF-81F-2R, FWF-81F-2R-3G4G-POE, FWF-81F-2R-POE FortiGate VM: FortiGate-ARM64-AWS, FortiGate-ARM64-KVM, FortiGate-ARM64-OCI, FortiGate-VM64, FortiGate-VM64-ALI, FortiGate-VM64-AWS, FortiGate-VM64-Azure, FortiGate-VM64-GCP, FortiGate-VM64-HV, FortiGate-VM64-IBM, FortiGate-VM64-KVM, FortiGate-VM64-OPC, FortiGate-VM64-RAXONDEMAND, FortiGate-VM64-XEN, FortiGate-VMX-Service-Manager FortiOS-VM: FOS-VM64, FOS-VM64-HV, FOS-VM64-KVM, FOS-VM64-Xen FortiGate Rugged: FGR-60F, FGR-60F-3G4G	7.0

FortiGate special branch models

The following FortiGate models are released on special branches of FortiOS. FortiManager version 7.4.1 supports these models on the identified FortiOS version and build number.

For information about supported FortiGate models released with FortiOS firmware, see [FortiGate models on page 24](#).

FortiOS 7.2

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-3200F	7.2.5	4373
FortiGate-3201F	7.2.5	4384
FortiGate-3700F, FortiGate-3701F	7.2.5	4394
FortiGate-4800F, FortiGate-4801F	7.2.5	4394

FortiOS 7.0

FortiGate Model	FortiOS Version	FortiOS Build
FortiGate-80F-DSL	7.0.12	6689
FortiGate-900G, FortiGate-901G	7.0.12	6728
FortiGate-1000F, FortiGate-1001F	7.0.12	6660
FortiGate-1500G, FortiGate-1501G	7.0.9	6458
FortiGate-3200F, FortiGate-3201F	7.0.12	6661
FortiGate-3700F, FortiGate-3701F	7.0.12	6661
FortiGate-4800F, FortiGate-4801F	7.0.12	6661
FortiGate-6000F, FortiGate-6300F, FortiGate-6300F-DC, FortiGate-6301F, FortiGate-6301F-DC, FortiGate-6500F, FortiGate-6500F-DC, FortiGate-6501F, FortiGate-6501F-DC	7.0.12	0163
FortiGate-7000E, FortiGate-7030E, FortiGate-7040E, FortiGate-7060E, FortiGate-7060E-8-DC	7.0.12	0163
FortiGate-7000F, FortiGate-7081F, FortiGate-7121F, FortiGate-7121F-2, FortiGate-7121F-2-DC, FortiGate-7121F-DC	7.0.12	0163
FortiGateRugged-70F, FortiGateRugged- 70F-3G4G	7.0.12	6668

FortiCarrier models

The following FortiCarrier models are released with FortiCarrier firmware.

For information about supported FortiCarrier models on special branch releases of FortiCarrier firmware, see [FortiCarrier special branch models on page 30](#).

Model	Firmware Version
FortiCarrier: FortiCarrier-2600F, FortiCarrier-2601F, FortiCarrier-3000D, FortiCarrier-3000F, FortiCarrier-3001F, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3300E, FortiCarrier-3301E, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3500F, FortiCarrier-3501F, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3960E, FortiCarrier-3980E, FortiCarrier-4200F, FortiCarrier-4201F, FortiCarrier-4400F, FortiCarrier-4401F FortiCarrier 5000 Series: FortiCarrier-5001E, FortiCarrier-5001E1 FortiCarrier 6000 Series: FortiCarrier-6000F, FortiCarrier-6300F, FortiCarrier-6300F-DC, FortiCarrier-6301F, FortiCarrier-6301F-DC, FortiCarrier-6500F, FortiCarrier-6500F-DC, FortiCarrier-65001F, FortiCarrier-6501F-DC FortiCarrier 7000 Series: FortiCarrier-7000E, FortiCarrier-7000F, FortiCarrier-7030E, FortiCarrier-7040E, FortiCarrier-7060E, FortiCarrier-7060E-8-DC, FortiCarrier-7081F, FortiCarrier-7121F, FortiCarrier-7121F-2, FortiCarrier-7121F-2-DC, FortiCarrier-7121F-DC FortiCarrier-DC: FortiCarrier-3000D-DC, FortiCarrier-3000F-DC, FortiCarrier-3001F-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3600E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3960E-DC, FortiCarrier-3980E-DC, FortiCarrier-4200F-DC, FortiCarrier-4201F-DC, FortiCarrier-4400F-DC, FortiCarrier-4401F-DC FortiCarrier-VM: FortiCarrier-ARM64-AWS, FortiCarrier-ARM64-Azure, FortiCarrier-ARM64-GCP, FortiCarrier-ARM64-KVM, FortiCarrier-ARM64-OCI, FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-KVM, FortiCarrier-VM64-IBM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	7.4
FortiCarrier: FortiCarrier-2600F, FortiCarrier-2601F, FortiCarrier-3000D, FortiCarrier-3000F, FortiCarrier-3001F, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3300E, FortiCarrier-3301E, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3500F, FortiCarrier-3501F, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3960E, FortiCarrier-3980E, FortiCarrier-4200F, FortiCarrier-4201F, FortiCarrier-4400F, FortiCarrier-4401F FortiCarrier 5000 Series: FortiCarrier-5001E, FortiCarrier-5001E1 FortiCarrier 6000 Series: FortiCarrier-6000F, FortiCarrier-6300F, FortiCarrier-6300F-DC, FortiCarrier-6301F, FortiCarrier-6301F-DC, FortiCarrier-6500F, FortiCarrier-6500F-DC, FortiCarrier-65001F, FortiCarrier-6501F-DC FortiCarrier 7000 Series: FortiCarrier-7000E, FortiCarrier-7000F, FortiCarrier-7030E, FortiCarrier-7040E, FortiCarrier-7060E, FortiCarrier-7060E-8-DC, FortiCarrier-7081F, FortiCarrier-7121F, FortiCarrier-7121F-2, FortiCarrier-7121F-2-DC, FortiCarrier-7121F-DC FortiCarrier-DC: FortiCarrier-3000D-DC, FortiCarrier-3000F-DC, FortiCarrier-3001F-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3600E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3960E-DC, FortiCarrier-3980E-DC, FortiCarrier-4200F-DC, FortiCarrier-4201F-DC, FortiCarrier-4400F-DC, FortiCarrier-4401F-DC	7.2

Model	Firmware Version
FortiCarrier-VM: FortiCarrier-ARM64-AWS, FortiCarrier-ARM64-Azure, FortiCarrier-ARM64-GCP, FortiCarrier-ARM64-KVM, FortiCarrier-ARM64-OCI, FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-IBM, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen	
FortiCarrier: FortiCarrier-3000D, FortiCarrier-3100D, FortiCarrier-3200D, FortiCarrier-3300E, FortiCarrier-3301E, FortiCarrier-3400E, FortiCarrier-3401E, FortiCarrier-3500F, FortiCarrier-3501F, FortiCarrier-3600E, FortiCarrier-3601E, FortiCarrier-3700D, FortiCarrier-3800D, FortiCarrier-3810D, FortiCarrier-3815D, FortiCarrier-3960E, FortiCarrier-3980E FortiCarrier 5000 Series: FortiCarrier-5001D, FortiCarrier-5001E, FortiCarrier-5001E1 FortiCarrier-DC: FortiCarrier-3000D-DC, FortiCarrier-3000F-DC, FortiCarrier-3001F-DC, FortiCarrier-3100D-DC, FortiCarrier-3200D-DC, FortiCarrier-3400E-DC, FortiCarrier-3401E-DC, FortiCarrier-3600E-DC, FortiCarrier-3700D-DC, FortiCarrier-3800D-DC, FortiCarrier-3810D-DC, FortiCarrier-3815D-DC, FortiCarrier-3960E-DC, FortiCarrier-3980E-DC FortiCarrier-VM: FortiCarrier-ARM64-AWS, FortiCarrier-ARM64-KVM, FortiCarrier-ARM64-OCI, FortiCarrier-VM64, FortiCarrier-VM64-ALI, FortiCarrier-VM64-AWS, FortiCarrier-VM64-Azure, FortiCarrier-VM64-GCP, FortiCarrier-VM64-HV, FortiCarrier-VM64-IBM, FortiCarrier-VM64-KVM, FortiCarrier-VM64-OPC, FortiCarrier-VM64-Xen, FortiCarrier-ARM64-KVM	7.0

FortiCarrier special branch models

The following FortiCarrier models are released on special branches of FortiOS Carrier. FortiManager version 7.4.1 supports these models on the identified FortiOS Carrier version and build number.

For information about supported FortiCarrier models released with FortiOS Carrier firmware, see [FortiCarrier models on page 28](#).

FortiCarrier 7.2

FortiCarrier Model	FortiCarrier Version	FortiCarrier Build
FortiCarrier-3200F	7.2.5	4373
FortiCarrier-3201F	7.2.5	4384
FortiCarrier-3700F, FortiCarrier-3701F	7.2.5	4394
FortiCarrier-4800F, FortiCarrier-4801F	7.2.5	4394

FortiCarrier 7.0

FortiCarrier Model	FortiCarrier Version	FortiCarrier Build
FortiCarrier-3200F, FortiCarrier-3201F	7.0.12	6661

FortiCarrier Model	FortiCarrier Version	FortiCarrier Build
FortiCarrier-3700F, FortiCarrier-3701F	7.0.12	6661
FortiCarrier-4800F, FortiCarrier-4801F	7.0.12	6661
FortiCarrier-6000F, FortiCarrier-6300F, FortiCarrier-6300F-DC, FortiCarrier-6301F, FortiCarrier-6301F-DC, FortiCarrier-6500F, FortiCarrier-6500F-DC, FortiCarrier-65001F, FortiCarrier-6501F-DC	7.0.12	0163
FortiCarrier-7000E, FortiCarrier-7030E, FortiCarrier-7040E, FortiCarrier-7060E, FortiCarrier-7060E-8-DC	7.0.12	0163
FortiCarrier-7000F, FortiCarrier-7081F, FortiCarrier-7121F, FortiCarrier-7121F-2, FortiCarrier-7121F-2-DC, FortiCarrier- 7121F-DC	7.0.12	0163

FortiADC models

Model	Firmware Version
FortiADC: FortiADC-100F, FortiADC-120F, FortiADC-200D, FortiADC-200F, FortiADC-220F, FortiADC-300D, FortiADC-300F, FortiADC-400D, FortiADC-400F, FortiADC-700D, FortiADC-1000F, FortiADC-1200F, FortiADC-1500D, FortiADC-2000D, FortiADC-2000F, FortiADC-2200F, FortiADC-4000D, FortiADC-4000F, FortiADC-4200F, FortiADC-5000F FortiADC VM: FortiADC-VM	7.1, 7.2, 7.4

FortiAnalyzer models

Model	Firmware Version
FortiAnalyzer: FortiAnalyzer-150G, FortiAnalyzer-300F, FortiAnalyzer-300G, FortiAnalyzer-400E, FortiAnalyzer-800F, FortiAnalyzer-800G, FortiAnalyzer-1000F, FortiAnalyzer-2000E, FortiAnalyzer-3000F, FortiAnalyzer-3000G, FortiAnalyzer-3500E, FortiAnalyzer-3500F, FortiAnalyzer-3500G, FortiAnalyzer-3700F, FortiAnalyzer-3700G, FortiAnalyzer-3900E FortiAnalyzer VM: FortiAnalyzer-DOCKER, FortiAnalyzer-VM64, FortiAnalyzer-VM64-ALI, FortiAnalyzer-VM64-AWS, FortiAnalyzer-VM64-AWS-OnDemand, FortiAnalyzer-VM64-Azure, FortiAnalyzer-VM64-Azure-OnDemand, FortiAnalyzer-VM64-GCP, FortiAnalyzer-VM64-HV, FortiAnalyzer-VM64-IBM, FortiAnalyzer-VM64-KVM, FortiAnalyzer-VM64-OPC, FortiAnalyzer-VM64-Xen	7.4

Model	Firmware Version
FortiAnalyzer: FortiAnalyzer-150G, FortiAnalyzer-300F, FortiAnalyzer-300G, FortiAnalyzer-400E, FortiAnalyzer-800F, FortiAnalyzer-800G, FortiAnalyzer-1000F, FortiAnalyzer-2000E, FortiAnalyzer-3000E, FortiAnalyzer-3000F, FortiAnalyzer-3000G, FortiAnalyzer-3500E, FortiAnalyzer-3500F, FortiAnalyzer-3500G, FortiAnalyzer-3700F, FortiAnalyzer-3700G, FortiAnalyzer-3900E FortiAnalyzer VM: FortiAnalyzer-DOCKER, FortiAnalyzer-VM64, FortiAnalyzer-VM64-ALI, FortiAnalyzer-VM64-AWS, FortiAnalyzer-VM64-AWS-OnDemand, FortiAnalyzer-VM64-Azure, FortiAnalyzer-VM64-Azure-OnDemand, FortiAnalyzer-VM64-GCP, FortiAnalyzer-VM64-HV, FortiAnalyzer-VM64-IBM, FortiAnalyzer-VM64-KVM, FortiAnalyzer-VM64-OPC, FortiAnalyzer-VM64-Xen	7.2
FortiAnalyzer: FortiAnalyzer-150G, FortiAnalyzer-200F, FortiAnalyzer-300F, FortiAnalyzer-300G, FortiAnalyzer-400E, FortiAnalyzer-800F, FortiAnalyzer-800G, FortiAnalyzer-1000F, FortiAnalyzer-2000E, FortiAnalyzer-3000E, FortiAnalyzer-3000F, FortiAnalyzer-3000G, FortiAnalyzer-3500E, FortiAnalyzer-3500F, FortiAnalyzer-3500G, FortiAnalyzer-3700F, FortiAnalyzer-3700G, FortiAnalyzer-3900E FortiAnalyzer VM: FortiAnalyzer-DOCKER, FortiAnalyzer-VM64, FortiAnalyzer-VM64-ALI, FortiAnalyzer-VM64-ALI-OnDemand, FortiAnalyzer-VM64-AWS, FortiAnalyzer-VM64-Azure, FortiAnalyzer-VM64-Azure-OnDemand, FortiAnalyzer-VM64-GCP, FortiAnalyzer-VM64-GCP-OnDemand, FortiAnalyzer-VM64-HV, FortiAnalyzer-VM64-IBM, FortiAnalyzer-VM64-KVM, FortiAnalyzer-VM64-OPC, FortiAnalyzer-VM64-Xen	7.0

FortiAnalyzer-BigData models

Model	Firmware Version
FortiAnalyzer-BigData: FortiAnalyzer-BigData-4500F FortiAnalyzer-BigData VM: FortiAnalyzer-BigData-VM64	7.2
FortiAnalyzer-BigData: FortiAnalyzer-BigData-4500F FortiAnalyzer-BigData VM: FortiAnalyzer-BigData-VM64	7.0

FortiAuthenticator models

Model	Firmware Version
FortiAuthenticator: FAC-200E, FAC-300F, FAC-400E, FAC-800F, FAC-2000E, FAC-3000E, FAC-3000F FortiAuthenticator VM: FAC-VM	6.5
FortiAuthenticator: FAC-200D, FAC-200E, FAC-300F, FAC-400C, FAC-400E, FAC-800F, FAC-1000C, FAC-1000D, FAC-2000E, FAC-3000D, FAC-3000E, FAC-3000F FortiAuthenticator VM: FAC-VM	6.4
FortiAuthenticator: FAC-200D, FAC-200E, FAC-300F, FAC-400C, FAC-400E, FAC-800F, FAC-1000C, FAC-1000D, FAC-2000E, FAC-3000D, FAC-3000E	6.3

Model	Firmware Version
FortiAuthenticator VM: FAC-VM	

FortiCache models

Model	Firmware Version
FortiCache: FCH-400C, FCH-400E, FCH-1000C, FCH-1000D, FCH-3000C, FCH-3000D, FCH-3000E, FCH-3900E FortiCache VM: FCH-KVM, FCH-VM64	4.1, 4.2
FortiCache: FCH-400C, FCH-400E, FCH-1000C, FCH-1000D, FCH-3000C, FCH-3000D, FCH-3900E FortiCache VM: FCH-VM64	4.0

FortiDDoS models

Model	Firmware Version
FortiDDoS: FortiDDoS-200F, FortiDDoS-1500F, FortiDDoS-2000F, FortiDDoS-3000F FortiDDoS VM: FortiDDoS-VM	6.5
FortiDDoS: FortiDDoS-200F, FortiDDoS-1500F, FortiDDoS-2000F, FortiDDoS-3000F FortiDDoS VM: FortiDDoS-VM	6.4
FortiDDoS: FortiDDoS-200F, FortiDDoS-1500F, FortiDDoS-2000F FortiDDoS VM: FortiDDoS-VM	6.3

FortiDeceptor models

Model	Firmware Version
FortiDeceptor: FDC-100G, FDC-1000F, FDC-1000G FortiDeceptor Rugged: FDCR-100G FortiDeceptor VM: FDC-VM	5.0, 5.1
FortiDeceptor: FDC-1000F, FDC-1000G FortiDeceptor Rugged: FDCR-100G FortiDeceptor VM: FDC-VM	4.3

FortiFirewall models

Some of the following FortiFirewall models are released on special branches of FortiFirewall firmware. FortiManager version 7.4.1 supports these models on the identified FortiFirewall firmware version and build number.

FortiFirewall 7.4

Model	Firmware Version
FortiFirewall: FortiFirewall-3980E	7.4
FortiFirewall DC: FortiFirewall-3980E-DC	
FortiFirewall-VM: FortiFirewall-VM64, FortiFirewall-VM64-KVM	7.4

FortiFirewall 7.2

Model	Firmware Version
FortiFirewall: FortiFirewall-3980E	7.2
FortiFirewall-VM: FortiFirewall-VM64, FortiFirewall-VM64-KVM	

FortiFirewall 7.0

Model	Firmware Version	Firmware Build (for special branch)
FortiFirewall: FortiFirewall-3001F	7.0.10	4955
FortiFirewall: FortiFirewall-3501F	7.0.10	4955
FortiFirewall: FortiFirewall-3980E	7.0	
FortiFirewall DC: FortiFirewall-3980E-DC		
FortiFirewall-VM: FortiFirewall-VM64		

FortiFirewallCarrier models

Some of the following FortiFirewallCarrier models are released on special branches of FortiFirewallCarrier firmware. FortiManager version 7.4.1 supports these models on the identified FortiFirewallCarrier firmware version and build number.

Model	Firmware Version	Firmware Build
FortiFirewallCarrier-VM: FortiFirewallCarrier-VM64, FortiFirewallCarrier-VM64-KVM	7.4	
FortiFirewallCarrier: FortiFirewallCarrier-3001F	7.0.10	4955
FortiFirewallCarrier: FortiFirewallCarrier-3501F	7.0.10	4940
FortiFirewallCarrier: FortiFirewallCarrier-4200F, FortiFirewallCarrier-4400F	6.4	

Model	Firmware Version	Firmware Build
FortiFirewallCarrier: FortiFirewallCarrier-4200F, FortiFirewallCarrier-4400F	6.2.7	5148
FortiFirewallCarrier: FortiFirewallCarrier-4401F	6.4.12	5423

FortiMail models

Model	Firmware Version
FortiMail: FE-200F, FE-400F, FE-900F, FE-2000E, FE-2000F, FE-3000E, FE-3000F, FE-3200E FortiMail VM: FML-VM	7.4
FortiMail: FE-60D, FE-200D, FE-200E, FE-200F, FE-400E, FE-400F, FE-900F, FE-2000E, FE-2000F, FE-3000E, FE-3000F, FE-3200E FortiMail VM: FML-VM	7.2
FortiMail: FE-60D, FE-200D, FE-200E, FE-200F, FE-400E, FE-400F, FE-900F, FE-1000D, FE-2000E, FE-2000F, FE-3000D, FE-3000E, FE-3000F, FE-3200E FortiMail VM: FML-VM	7.0

FortiPAM models

Model	Firmware Version
FortiPAM: FortiPAM-1000G, FortiPAM-3000G FortiPAM VM: FortiPAM-Azure, FortiPAM-HyperV, FortiPAM-KVM, FortiPAM-VM64	1.0, 1.1

FortiProxy models

Model	Firmware Version
FortiProxy: FPX-400E, FPX-2000E, FPX-4000E FortiProxy VM: FortiProxy-AliCloud, FortiProxy-AWS, FortiProxy-Azure, FortiProxy-GCP, FortiProxy-HyperV, FortiProxy-KVM, FortiProxy-VM64	7.2, 7.4
FortiProxy: FPX-400E, FPX-400G, FPX-2000E, FPX-2000G, FPX-4000E, FPX-4000G FortiProxy VM: FortiProxy-AliCloud, FortiProxy-AWS, FortiProxy-Azure, FortiProxy-GCP, FortiProxy-HyperV, FortiProxy-KVM, FortiProxy-VM64	7.0
FortiProxy: FPX-400E, FPX-2000E, FPX-4000E FortiProxy VM: FortiProxy-KVM, FortiProxy-VM64	1.0, 1.1, 1.2, 2.0

FortiSandbox models

Model	Firmware Version
FortiSandbox: FSA-500F, FSA-500G, FSA-1000D, FSA-1000F, FSA-1500G, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3000F, FSA-3500D FortiSandbox DC: FSA-1000F-DC FortiSandbox-VM: FortiSandbox-AWS, FortiSandbox-Cloud, FSA-VM	4.2
FortiSandbox: FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3000F, FSA-3500D FortiSandbox DC: FSA-1000F-DC FortiSandbox-VM: FortiSandbox-AWS, FortiSandbox-Cloud, FSA-VM	4.0
FortiSandbox: FSA-500F, FSA-1000D, FSA-1000F, FSA-2000E, FSA-3000D, FSA-3000E, FSA-3500D FortiSandbox DC: FSA-1000F-DC FortiSandbox-VM: FortiSandbox-AWS, FSA-VM	3.2

FortiSOAR models

Model	Firmware Version
FortiSOAR VM: FortiSOAR-VM	7.2, 7.3, 7.4

FortiSwitch ATCA models

Model	Firmware Version
FortiController: FTCL-5103B, FTCL-5903C, FTCL-5913C	5.2
FortiSwitch-ATCA: FS-5003A, FS-5003B FortiController: FTCL-5103B	5.0
FortiSwitch-ATCA: FS-5003A, FS-5003B	4.3

FortiTester models

Model	Firmware Version
FortiTester: FortiTester-100F, FortiTester-2000D, FortiTester-2000E, FortiTester-2000F, FortiTester-2500E, FortiTester-3000E, FortiTester-4000E	7.2

Model	Firmware Version
FortiTester VM: FortiTester-VM, FortiTester-VM-ALI-BYOL, FortiTester-VM-ALI-PAYG, FortiTester-VM-AWS-BYOL, FortiTester-VM-AWS-PAYG, FortiTester-VM-AZURE-BYOL, FortiTester-VM-AZURE-PAYG, FortiTester-VM-GCP-BYOL, FortiTester-VM-GCP-PAYG, FortiTester-VM-IBM-PAYG, FortiTester-VM-KVM, FortiTester-VM-OCI-BYOL, FortiTester-VM-OCI-PAYG	
FortiTester: FortiTester-60F, FortiTester-100F, FortiTester-2000D, FortiTester-2000E, FortiTester-2000F, FortiTester-2500E, FortiTester-3000E, FortiTester-3000F, FortiTester-4000E, FortiTester-4000F FortiTester VM: FortiTester-VM, FortiTester-VM-ALI-BYOL, FortiTester-VM-ALI-PAYG, FortiTester-VM-AWS-BYOL, FortiTester-VM-AWS-PAYG, FortiTester-VM-AZURE-BYOL, FortiTester-VM-AZURE-PAYG, FortiTester-VM-GCP-BYOL, FortiTester-VM-GCP-PAYG, FortiTester-VM-IBM-PAYG, FortiTester-VM-KVM, FortiTester-VM-OCI-BYOL, FortiTester-VM-OCI-PAYG	7.1
FortiTester: FortiTester-60F, FortiTester-100F, FortiTester-2000D, FortiTester-2000E, FortiTester-2000F, FortiTester-2500E, FortiTester-3000E, FortiTester-3000F, FortiTester-4000E, FortiTester-4000F FortiTester VM: FortiTester-VM, FortiTester-VM-ALI-BYOL, FortiTester-VM-ALI-PAYG, FortiTester-VM-AWS-BYOL, FortiTester-VM-AWS-PAYG, FortiTester-VM-AZURE-BYOL, FortiTester-VM-AZURE-PAYG, FortiTester-VM-GCP-BYOL, FortiTester-VM-GCP-PAYG, FortiTester-VM-IBM-PAYG, FortiTester-VM-KVM, FortiTester-VM-OCI-BYOL, FortiTester-VM-OCI-PAYG	7.0

FortiWeb models

Model	Firmware Version
FortiWeb: FortiWeb-100D, FortiWeb-100E, FortiWeb-400C, FortiWeb-400D, FortiWeb-400E, FortiWeb-600D, FortiWeb-600E, FortiWeb-1000D, FortiWeb-1000E, FortiWeb-2000E, FortiWeb-2000F, FortiWeb-3000C, FortiWeb-3000CFSX, FortiWeb-3000D, FortiWeb-3000DFSX, FortiWeb-3000E, FortiWeb-3000F, FortiWeb-3010E, FortiWeb-4000C, FortiWeb-4000D, FortiWeb-4000E, FortiWeb-4000F FortiWeb VM: FortiWeb-Azure, FortiWeb-Azure_OnDemand, FortiWeb-Docker, FortiWeb-GCP, FortiWeb-GCP_OnDemand, FortiWeb-HyperV, FortiWeb-VM, FortiWeb-XENOpenSource, FortiWeb-XENServer	6.4, 7.0, 7.2

Resolved Issues

The following issues have been fixed in 7.4.1. To inquire about a particular bug, please contact [Customer Service & Support](#).

AP Manager

Bug ID	Description
861941	FortiManager attempts to install "arp-profile" even if "darp" is disabled.
892773	Assigning AP Profile returns invalid value.
906930	FortiManager displays an error for Subnets overlap for a Bridge SSID.

Device Manager

Bug ID	Description
768289	There is a discrepancy in the usage of quotation marks (") when configuring DHCP relay from FortiManager or retrieving it from FortiGate.
831624	<i>SD-WAN Monitor</i> under <i>Monitors</i> displays time frame as "invalid date - invalid date".
895001	The "gui-ztna" configuration is displayed as enabled on the FortiManager even though this setting is disabled on the FortiGate.
896367	The geographic coordination config of FortiGates on <i>Device Manager</i> is being reset to 0, 0 after a certain period of time.
899350	Promote button is missing for Fortigate 80F Clusters.
902908	Managed FortiAnalyzer is not listed under <i>System Template</i> .
906558	Importing a Revision fails and displays a runtime error.
909867	FortiManager attempts to configure unsupported syntax for "sdwan health-check".
910391	When FortiManager operates in a non-default workspace mode, it may attempt to purge the configuration of the FortiGate devices due to database corruption.
911535	Adding a Model device with MetaVariables changes the status of other devices which using the MetaVariables to Modified/unknown.
912833	Adding FortiGates with Open Authentication (OAuth) Method, Fortinet Security Fabric dialog

Bug ID	Description
	box does not display the FortiManager's related info.
915361	FortiWifi devices are displayed in FortiManager under the Vulnerable devices as FortiAP.
917969	FortiManager is unable to search static routes via its interface name.
918292	The SD-WAN services cannot be modified, and attempting to make changes results in an 'Invalid Value' error message.
919613	When using a space character in 'psksecret', the FMG is unable to install the 'psksecret' and displays an error message.
921094	In 6.2 or 6.4 ADOMs, problems might occur when attempting to add or modify static routes.
925546	Assigned Devices on Provisioning Template/CLI Template shows incorrect VDOM.
925684	Only a maximum of 10 devices can be previewed before installation using 'install preview'.
925854	FortiManager fails to load the security fabric data for FortiGates (Versions 7.0.5+ & 7.2.5).

FortiSwitch Manager

Bug ID	Description
881766	Event logs or task manager do not show which user authorized a FortiSwitch.
922068	<i>FortiSwitch Manager</i> does not display any ports for managed switches.
947651	Per Device under the <i>FortiSwitch Manager</i> cannot edit FortiSwitch name and GUI returns error "invalid value".

Global ADOM

Bug ID	Description
894714	FortiManager does not allow creating/modification or removing the per-device mapping in global objects in assigned ADOM.
906058	Firewall address cannot be deleted from Global ADOM; it displays an error message indicating that the object is being used in ADOM root.
925188	The per-device mapping for any assigned global objects cannot be modified.

Others

Bug ID	Description
671904	FortiManager does not support the "Lock Override" feature when Workspace mode works on Per-ADOM mode.
880465	TCP ports 8902 & 8903 are opened and in listening mode after the upgrade.
894947	FortiManager fails to trigger the event handler for its local events after enabling the FortiAnalyzer features.
895982	Admin with a super user profile is not able to create the Firmware Template when FortiManager is working in the Workflow mode.
897157	Unexpected changes in existing static routes, created by static route template after upgrade to 7.0.7, 7.2.2, 7.4.0.
910175	When provisioning the FortiExtender via CLI template, FortiManager displays the "mismatch interface" error message.
914027	FortiManager does not display/use the latest ISDB version for all of its ADOMs.
916463	The approval emails are not being sent to the "Email Notification" admins when a new session is created and submitted for approval.
917834	<i>Report Definitions</i> cannot be viewed or modified from FortiManager when FortiAnalyzer is being managed by FortiManager.
918129	FortiManager does not support the AWS Security Token Service in AWS SDN connector.
919088	GUI may not work properly in Google Chrome and Microsoft Edge version 114.
919981	Installation fails to Azure FortiGate standalone as FortiManager attempts to set the peervd to "root".
921273	Unable to upgrade ADOMs due to the XSS vulnerability characters check on wireless-controller.
925778	FortiGates are displayed offline and Inactive on FortiWLM MEA.
930305	Firmware template upgrade preview shows incorrect versions for the upgrade.
930425	When downloading the install preview, the file name doesn't include the timestamp.

Policy and Objects

Bug ID	Description
696367	Hit count, first used, and last used may not get updated on FortiManager.
780058	FortiManager's GUI does not support the "src-vendor-mac" objects in Firewall policy.

Bug ID	Description
830640	"Send files to FortiSandbox for inspection" option is being enabled when creating an antivirus profile.
863819	Unable to delete unused objects.
869863	NSX connector; unable to unselect the group with no users.
873358	Installation fails as FortiManager tries to set "cgn-client-startip" and "cgn-client-endip" settings when ippool object has been modified.
880418	The default values of the Application Control Profile entries cannot be changed.
883064	Any admin make changes to "Object Selection Pane", either set it to <i>Dock to Right</i> , <i>Dock to Bottom</i> , or <i>Classic Dual Pane</i> , it will affect all other admin's GUI preferences.
894597	Default value for "unsupported-ssl-version" in ssl-ssh-profile gets modified during the installation.
896461	FortiManager disables ip6-send-adv after opening and closing interface configuration.
896491	Installation fails with unclear error message: "vdom copy failed".
898883	Exported firewall policies do not contain firewall address values IP, netmask, and other details.
899135	Installation fails as FortiManager tries to unset the "arp-profile" during the installation.
902298	FortiManager does not generate error messages when invalid or obsolete application IDs are used in the policy. Instead, it allows installation and sets the category to 'pass' or 'monitor'.
908445	FortiManager does not display correct edit page for virtual server VIP when edit object in policy table.
911146	Under the <i>Policy & Objects</i> , GUI does not display the Address Object list.
911632	When retrieving the configuration from the FortiGate, the FortiManager shows the new cert; however, those can't be assigned to the FCT EMS connector.
912114	FortiManager is unable to import OpenStack SDN connector and the following error message is displayed: "send_sdn_connector_openstack_cmd: Failed to get openstack token".
914945	Unable to modify or clone the "SSL/SSH inspection profile" in the <i>Policy & Objects</i> on the ADOM 7.0 version.
914981	In <i>Policy & Objects</i> , local policy is not displayed if view mode " <i>Interface pair view</i> " is selected.
916459	The option 'Allow Websites When a Rating Error Occurs' is not being saved correctly in the default web filter.
919415	Unable to "Edit" and "Delete" Installation Target after enable classic dual pane mode.
919681	The incoming and outgoing interfaces are not loading after creating a custom policy package in a 7.2 FortiGate ADOM.
920740	Unable to create a per device mapping for a virtual server.
920983	The policy blocks using a group object do not get updated when the objects within the group

Bug ID	Description
	are modified.
922648	FortiManager unable to push WiFi SSID to FortiGates.
925058	"Web URL Filter" entries are not visible in the Web Filter Profile.
925076	FortiManager tries to install different preconnection-id under <i>VPN SSL WEB Portal > Profile > Bookmark-Group > Gui-Bookmark > Book</i> .

Revision History

Bug ID	Description
904710	Restoring a revision of a policy removes the information of all the SD-WAN rules.

Script

Bug ID	Description
913360	Device script is trying to add additional configuration; therefore, installation gets failed.
923966	When FortiManager is operating in Workspace mode, there are no options to save changes after executing a CLI script.
931196	Scheduled Scripts created by the LDAP users cannot be run and FortiManager displays "Data is not ready" error message.

System Settings

Bug ID	Description
733279	After changing the http or https port, FortiManager displays an "Unknown Error." error message.
842732	FortiManager does not display the Secondary HA member's status correctly.
861997	Unable to delete a particular non-default empty ADOM.
890956	SAML SSO Authentication only works with the default local certs.

VPN Manager

Bug ID	Description
863424	The "Latest Patch Level" should be available with action "Check-up-to-date" under the SSL VPN Portal.
931564	In <i>VPN Manager</i> , ipsec vpn map, topology view and traffic view does not display map normally.

Known Issues

The following issues have been identified in 7.4.1. To inquire about a particular bug or to report a bug, please contact [Customer Service & Support](#).

AP Manager

Bug ID	Description
884233	FortiManager displays the AP critical security vulnerability info even after FortiAPs are being upgraded.

Device Manager

Bug ID	Description
888948	The "firewall ssh setting" objects cannot be retrieved on FortiManager due to the FortiOS's bug (ID 0906987).
939921	The firmware upgrade in ADOM mode backup is not allowed.
948475	"View Diff" function under the <i>Device Manager > Device Configuration DB</i> per device does not function properly.

FortiSwitch Manager

Bug ID	Description
940419	When adding FortiSwitch on FortiManager, error message "Import error - invalid port number" is displayed.
945424	The FortiManager fails to install the created switch template to the FSW, displaying the error message 'VLAN XXX already exists.'

Others

Bug ID	Description
703585	FortiManager may return 'Connection aborted' error with JSON API request.
777831	When FortiAnalyzer is added as a managed device to FortiManager, " <i>Incident & Event</i> " will be displayed instead of the " <i>FortiSoC</i> ".
796858	Subject Key Identifier extension is missing on FortiManager ADOM CA certificate.
891253	The firmware upgrade is successful; however, the task line does not get updated for the retrieve action when device names exceed the predefined character limit.
922957	the "fmgd" process may crash while loading the ADOM when multiple Policy Packages are locked.
924164	The firmware template status changes to 'unknown' after retrieve.
935430	When FortiAnalyzer is managed by FortiManager and FortiManager's local logs are being sent to FortiAnalyzer, installing PP to FortiGates may display the following message: "Confirm Deletion FortiManager is going to sync the following device deletion to FortiAnalyzer,...".

Policy & Objects

Bug ID	Description
718223	Hyperscale firewall EIF shall not be enabled when IP pool with CGN overload configuration is used in a policy.
725427	Policy package install skips the policy where destination interface is set as SD-WAN zone and policy is IPSEC policy.
751443	FortiManager displays policy installation copy failures error when ipsec template gets unassigned. Workaround: Instead of unassigning IPSec template, modify IPSec template, replace the reference to IPSec tunnel interface with another interface. Please ensure a fresh FMG backup is created prior to any changes.
779363	FortiManager fails to install <code>analytics-wl-filetype</code> in AV profile to FortiGates.
845022	SDN Connector failed to import objects from VMware VSphere.
855073	The "where used" feature does not function properly.
855317	New users added to the user group for IPSec dial-up XAuth authentication do not get installed.
886911	FortiManager is attempting to modify replacement messages after upgrade, and this leads to installation failure.

Bug ID	Description
900229	In policy-based policy packaged, application IDs are displayed instead of their names.
907925	IPS profile/Signature tab is not visible for admins with non-default admin profile.
917471	The EMS connector is automatically being disabled.
938019	Policy Package Status not changed on modification of nested group used in policy block.

Revision History

Bug ID	Description
801614	FortiManager might display an error message "Failed to create a new revision." for some FortiGates, when retrieving their configurations.

System Settings

Bug ID	Description
825319	FortiManager fails to promote a FortiGate HA member (running on firmware 7.2.0 to 7.2.4) to the Primary.
853429	Creating FortiManager's configuration backup via scp cannot be done.

VPN Manager

Bug ID	Description
906097	VPN Manager IPsec community Phase 2 encryption setting can't be changed to AES256GCM from the GUI.

Appendix A - FortiGuard Distribution Servers (FDS)

In order for FortiManager to request and retrieve updates from FDS, and for FortiManager to serve as an FDS, please configure the necessary settings on all devices between FortiManager and FDS, or between FortiManager and FortiGate devices based on the following items:

- FortiManager accesses FDS for antivirus and attack updates through TCP/SSL port 443.
- If there is a proxy server between FortiManager and FDS, FortiManager uses port 80 to communicate with the proxy server by default, and connects to the proxy server using HTTP protocol.
- If FortiManager manages a FortiGate device located behind a proxy server, the proxy server permits TCP/SSL traffic to pass through port 443.

FortiGuard Center update support

You can configure FortiManager as a local FDS to provide FortiGuard updates to other Fortinet devices and agents on your network. The following table lists which updates are available per platform:

Platform	Update Service	Query Service
FortiGate	✓	✓
FortiADC	✓	
FortiCache	✓	
FortiCarrier	✓	✓
FortiClient	✓	
FortiDeceptor	✓	✓
FortiDDoS	✓	
FortiEMS	✓	
FortiMail	✓	✓
FortiProxy	✓	✓
FortiSandbox	✓	✓
FortiSOAR	✓	
FortiTester	✓	
FortiWeb	✓	

Appendix B - Default and maximum number of ADOMs supported

This section identifies the supported number of ADOMs for FortiManager hardware models and virtual machines.

Hardware models

FortiManager supports a default number of ADOMs based on hardware model.

Some hardware models support an ADOM subscription license. When you purchase an ADOM subscription license, you increase the number of supported ADOMs. For example, you can purchase an ADOM subscription license for the FMG-3000G series, which allows you to use up to a maximum of 8000 ADOMs.

Other hardware models do not support the ADOM subscription license. For hardware models that do not support the ADOM subscription license, the default and maximum number of ADOMs is the same.

FortiManager Platform	Default number of ADOMs	ADOM license support?	Maximum number of ADOMs
200G Series	30		30
300F Series	100		100
400G Series	150		150
1000F Series	1000		1000
2000E Series	1200		1200
3000G Series	4000	✓	8000
3700G Series	10,000	✓	12,000

For FortiManager F series and earlier, the maximum number of ADOMs is equal to the maximum devices/VDOMs as described in the [FortiManager Data Sheet](#).

Virtual Machines

FortiManager VM subscription license includes five (5) ADOMs. Additional ADOMs can be purchased with an ADOM subscription license.

For FortiManager VM perpetual license, the maximum number of ADOMs is equal to the maximum number of Devices/VDOMs listed in the [FortiManager Data Sheet](#).



FortiManager VM subscription and perpetual licenses are stackable.



www.fortinet.com

Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.